L2TPv3 VPN Technology and Applications

Ray Irani (rirani@cisco.com)

Cisco Systems, Inc.

APRICOT 2004 Conference , Feb.25-26, 2004

Agenda – L2TPv3

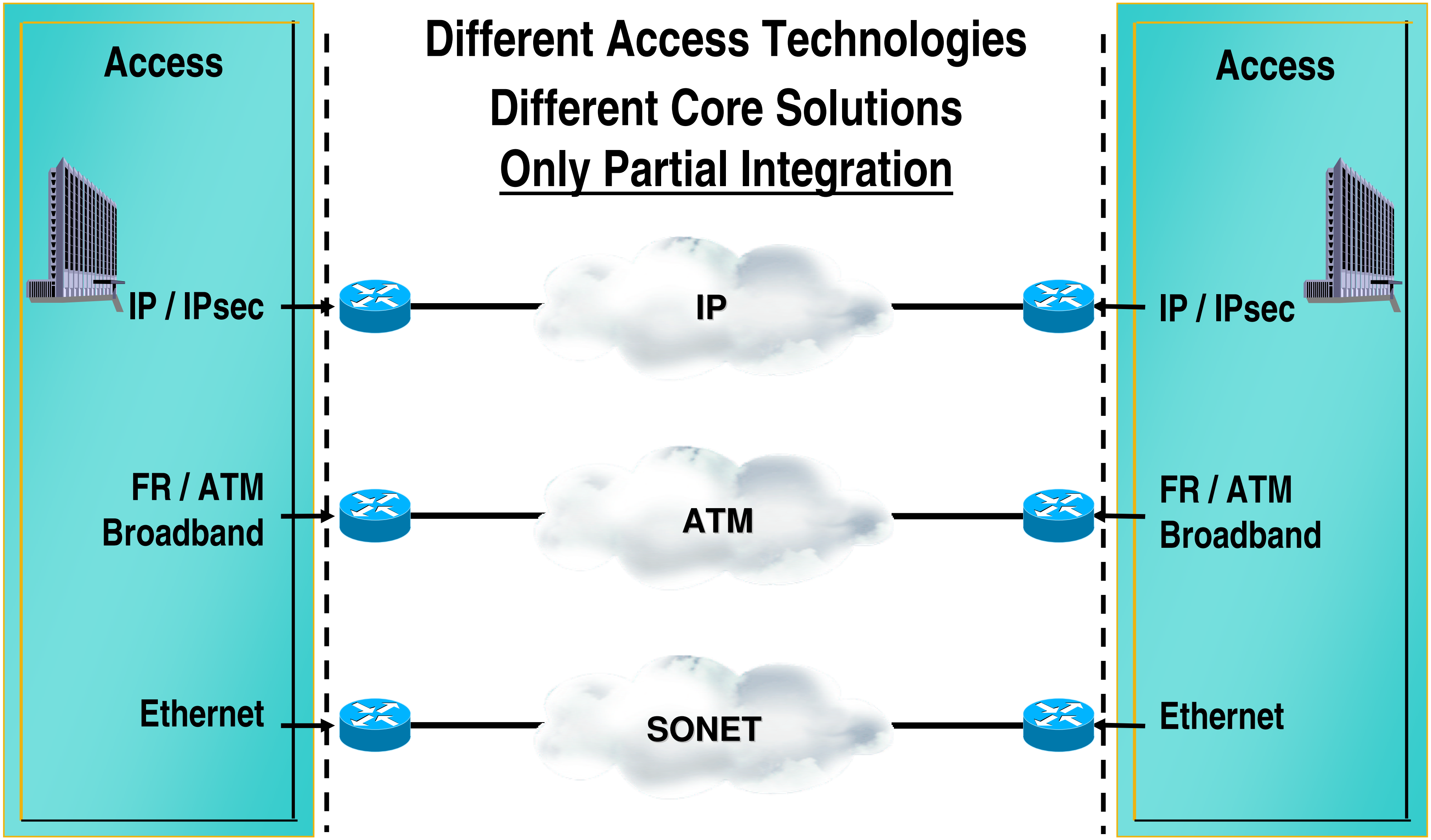
- Introduction
- Technology
- Applications
- References

VPN Deployments Today: Technology & VPN Diversity

Different Access Technologies

Different Core Solutions

Only Partial Integration

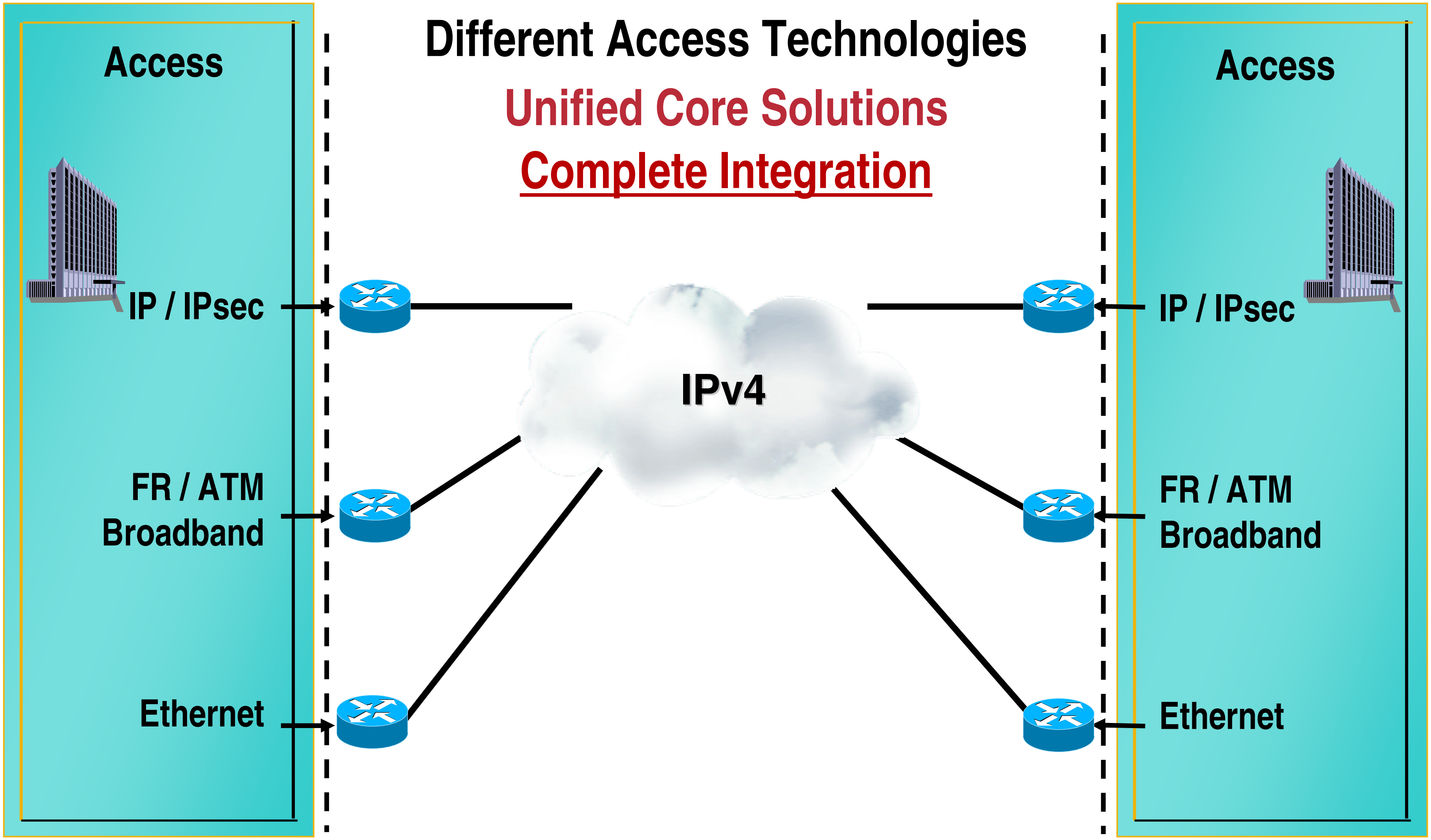


Deployments – Utilizing L2 Tunneling Technologies

Different Access Technologies

Unified Core Solutions

Complete Integration

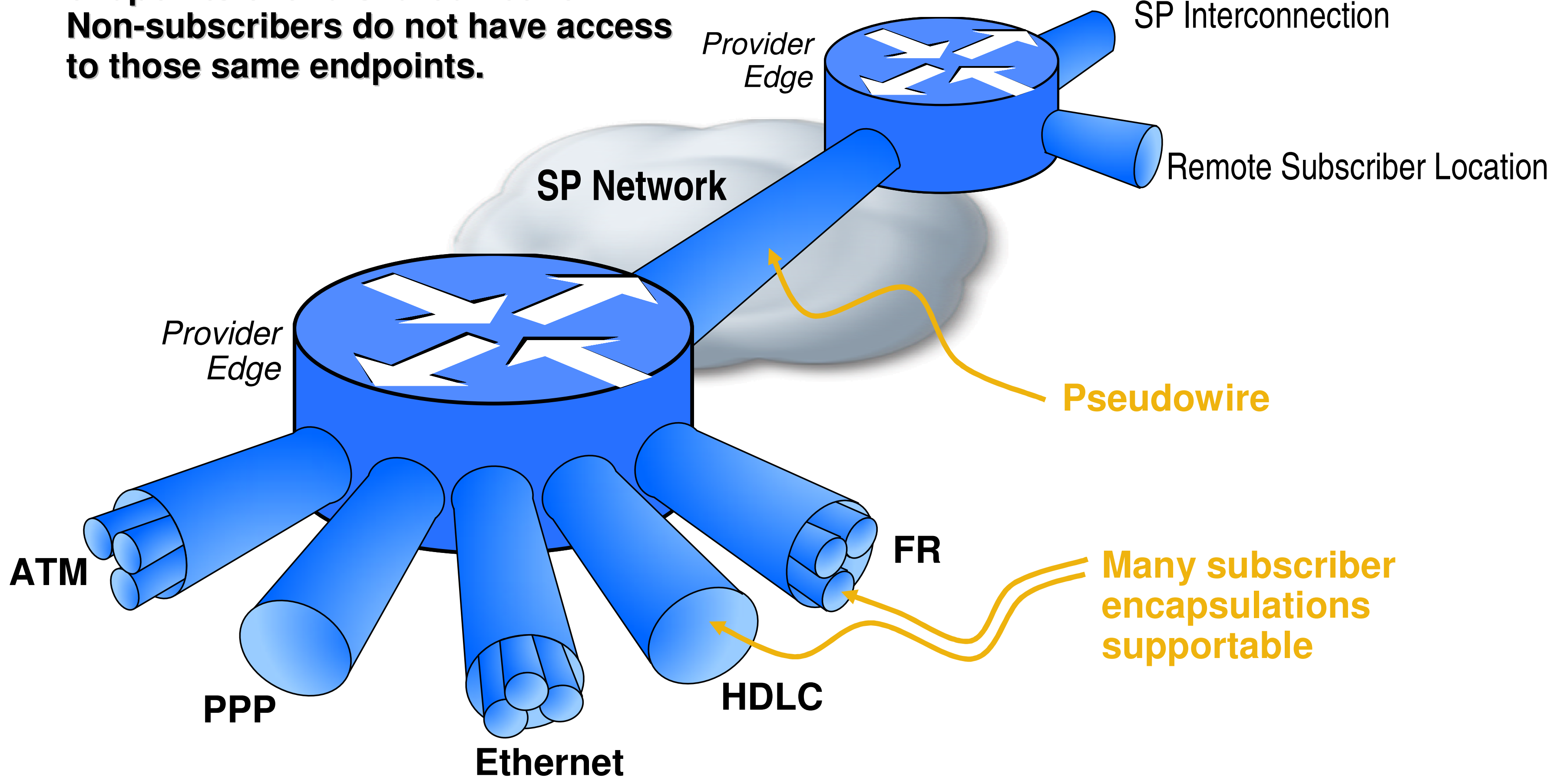


A Brief Word about L2 / L3 VPNs

Layer 3 VPNs	Layer 2 VPNs
• Provider devices forward customer packets based on Layer 3 information (e.g., IP)	• Provider devices forward customer packets based on Layer 2 information
• SP involvement in routing	• Tunnels, circuits, LSPs, MAC address
• MPLS/BGP VPNs (RFC 2547), GRE, virtual router approaches	• "pseudo-wire" concept

What Is an L2VPN?
IETF's L2VPN Logical Context

- **An L2VPN is comprised of switched connections between subscriber endpoints over a shared network. Non-subscribers do not have access to those same endpoints.**



Some L1 frame encapsulations are transportable under the framework of L2VPN. This is acceptable since (unlike native L1) Frames can be dropped due to congestion.

Agenda – L2TPv3

- Introduction
- Technology
- Applications
- References

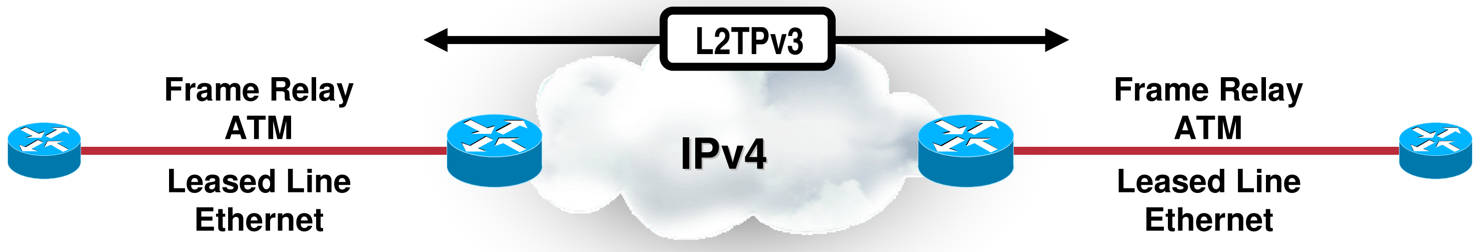
L2TPv3

Layer 2 Tunneling Protocol version 3

The Layer 2 Tunneling Protocol version 3 (L2TPv3) allows a pair of routers connected via an IP network to provide high-speed transparent Layer 2 connectivity between a pair of interfaces.

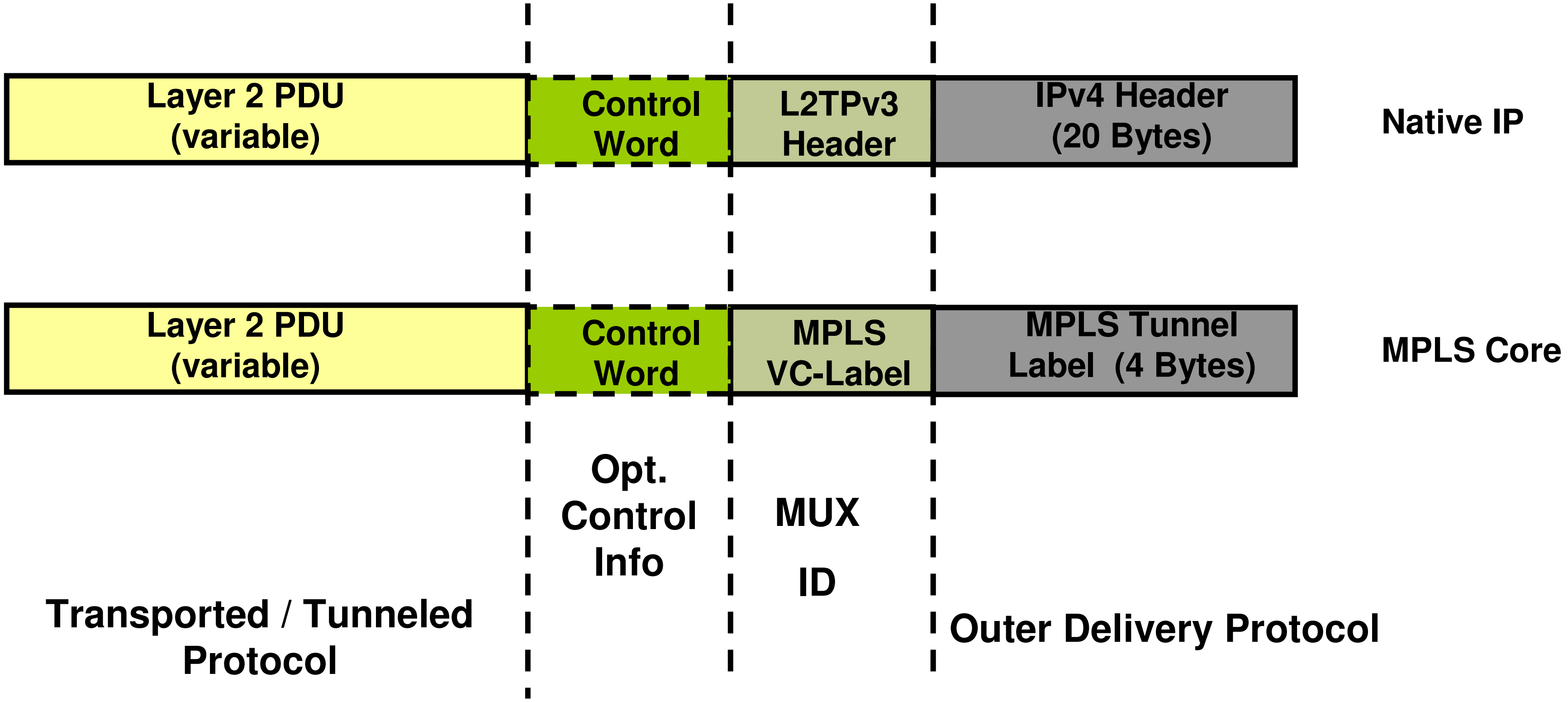
This functionality can be used to build Layer 2 VPNs or to support legacy network migration.

New IP Tunneling Protocol -
Layer 2 Tunneling Protocol Version 3 – L2TPv3



- L2TPv3 transports layer 2 traffic over an IP network
- Control Connection between edge routers for dynamic setup and maintenance of emulated circuits
- Based on a well-established lineage of protocols:
  - L2TPv2 and pre-standards Cisco innovation
- A standards track (IETF L2TPEXT WG) open architecture allows extensibility to many transport types
- Configuration on edge routers only
- Data plane provides session demultiplexing, sequencing, etc. for emulated circuits

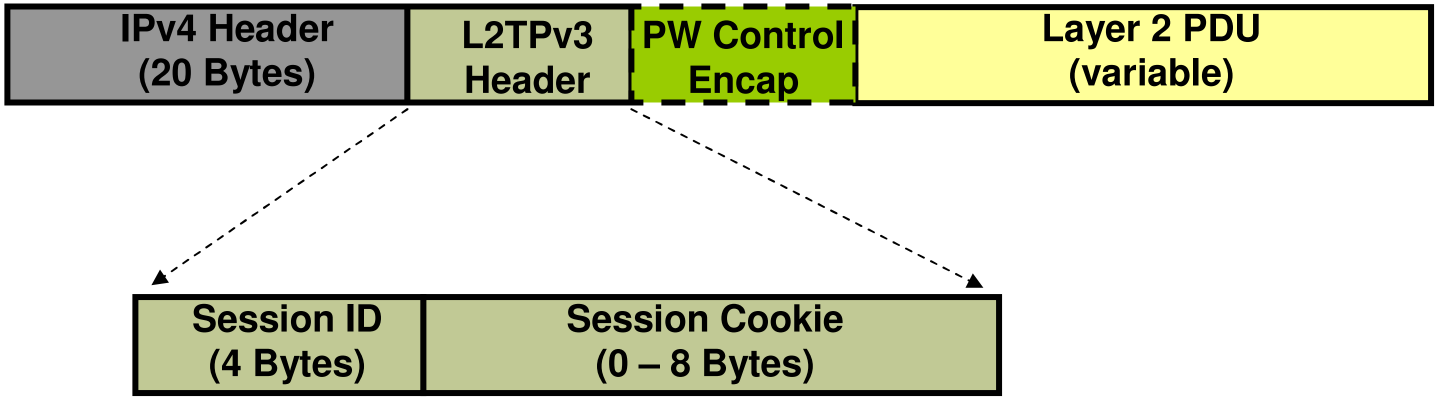
L2VPN – Data Messages



- **Both transport technologies have similar purposes, functionality and features.**

L2TPv3 – Data Messages

Data Plane



IPv4 Header - The delivery header for the Tunnel. Always destined for an LCCE.

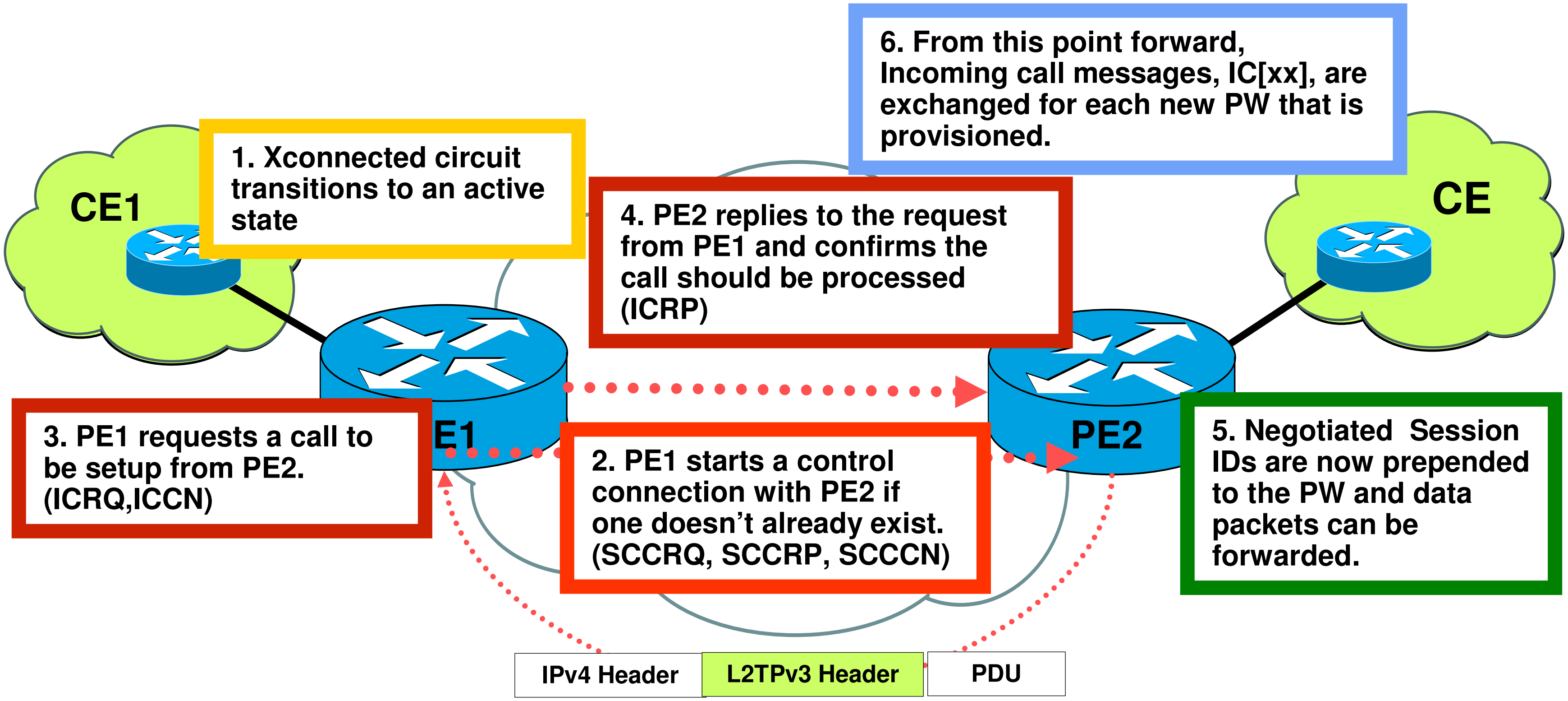
L2TPv3 header – Consists of two parts; (1) **Session ID** used to uniquely identify the correct Session on the Remote system, and (2) the **Cookie** used as an added measure of session integrity between peers.

L2 PW Control Encapsulation - Sequence numbers, priority bits, and any additional flags needed to support the L2 emulation for the given PW type. There is a default defined in the L2TPv3 base specification, though this may vary among PW types if necessary.

Payload - Payload to be transported by L2TPv3. Typically the entire link-level frame.

L2TPv3 – Control Connection and Session Negotiation

Control Plane



1. Xconnected circuit transitions to an active state

2. PE1 starts a control connection with PE2 if one doesn't already exist. (SCCRQ, SCCRP, SCCCN)

3. PE1 requests a call to be setup from PE2. (ICRQ,ICCN)

4. PE2 replies to the request from PE1 and confirms the call should be processed (ICRP)

5. Negotiated Session IDs are now prepended to the PW and data packets can be forwarded.

6. From this point forward, Incoming call messages, IC[xx], are exchanged for each new PW that is provisioned.

🟨 : Initiation

🟧 : Control Channel Establishment

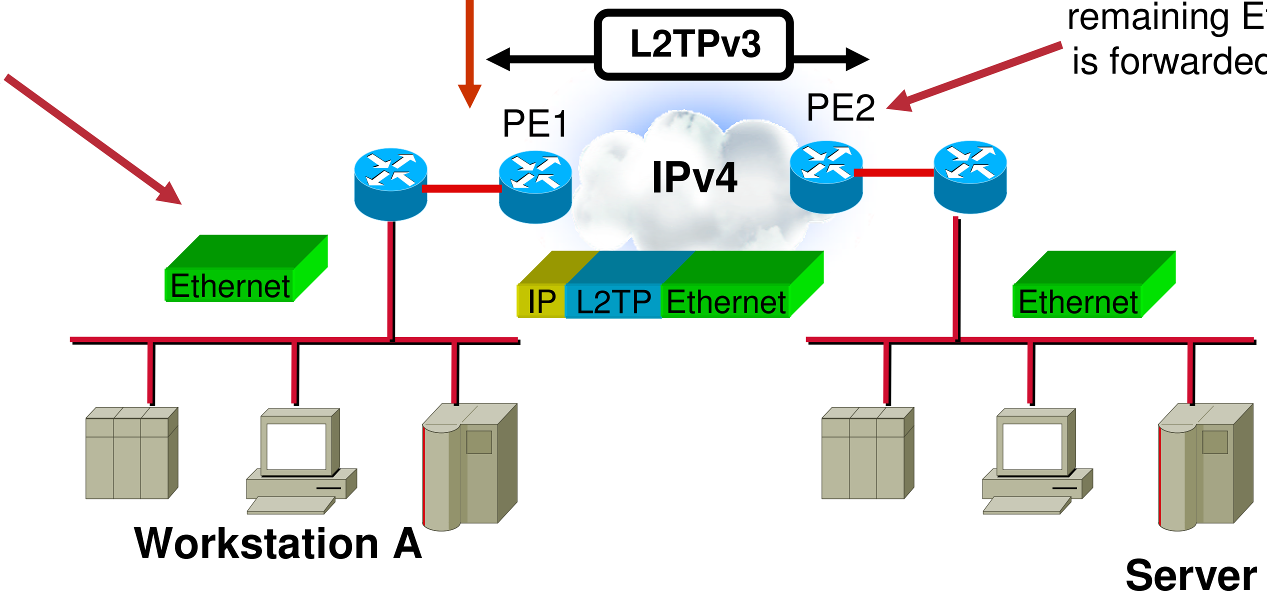
🟥 : Session ID Establishment for Data Plane

Bi-directional Session ID exchange initiated by one of the L2TP Control Connection Endpoints (LCCEs)

Agenda – L2TPv3

- Introduction
- Technology
- Applications
- References

L2TPv3 – Ethernet Application Overview



Step #1 Workstation A sends packet destined for Server B

Step #2 PE1 takes Ethernet frame and encapsulates its entirety in L2TP and routes it to tunnel destination

Step #3 PE2 receives IP/L2TP/Ethernet Packet and removes the IP/L2TPv3 headers. The remaining Ethernet frame is forwarded to Server B.

Two Ethernet Segments are joined over an IP core via L2TPv3. To the end user devices, the two physical Ethernet networks appear as a single segment.

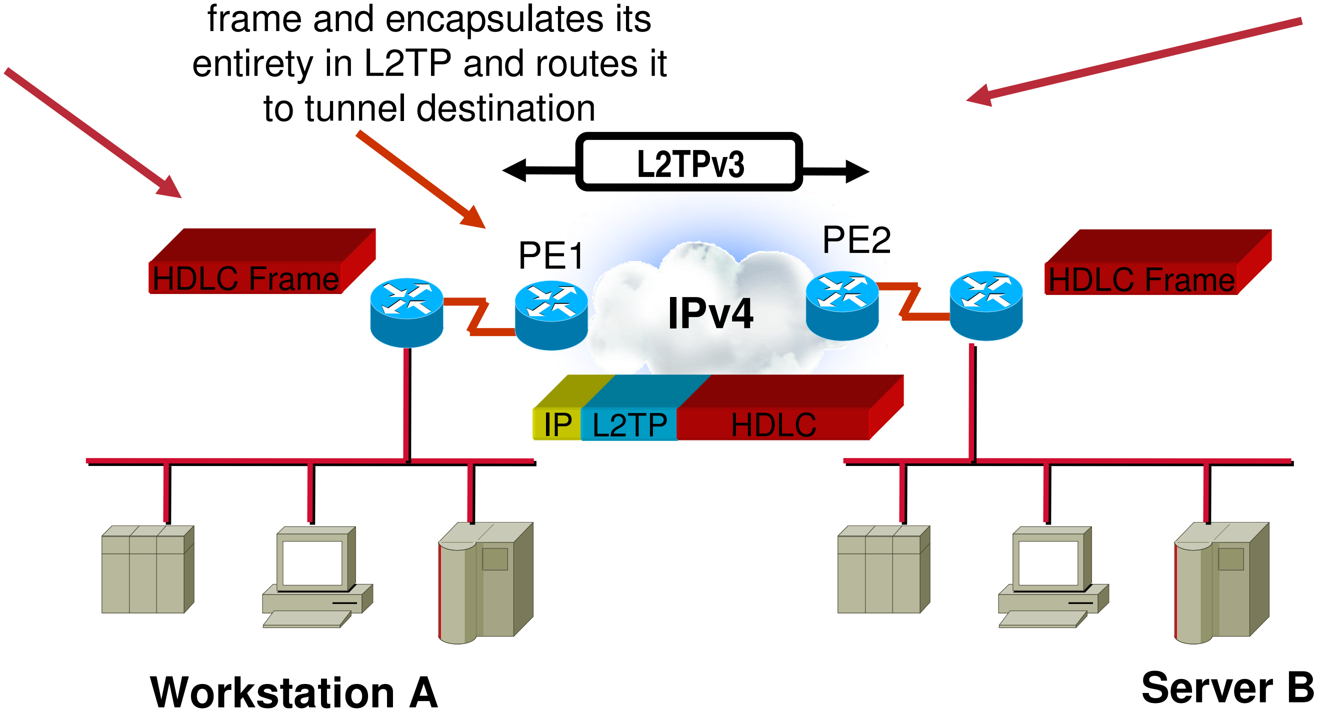
Note: Ethernet frame will be encap in its entirety with an L2TPv3 data header. At the other end, a received L2TPv3 data packet will be stripped of its L2TPv3 header.

L2TPv3 – Leased Application Overview

Step #1 Workstation A sends packet destined for Server B

Step #2 PE1 takes HDLC frame and encapsulates its entirety in L2TP and routes it to tunnel destination

Step #3 PE2 receives IP/L2TP/HDLC Packet and removes the IP/L2TPv3 headers.



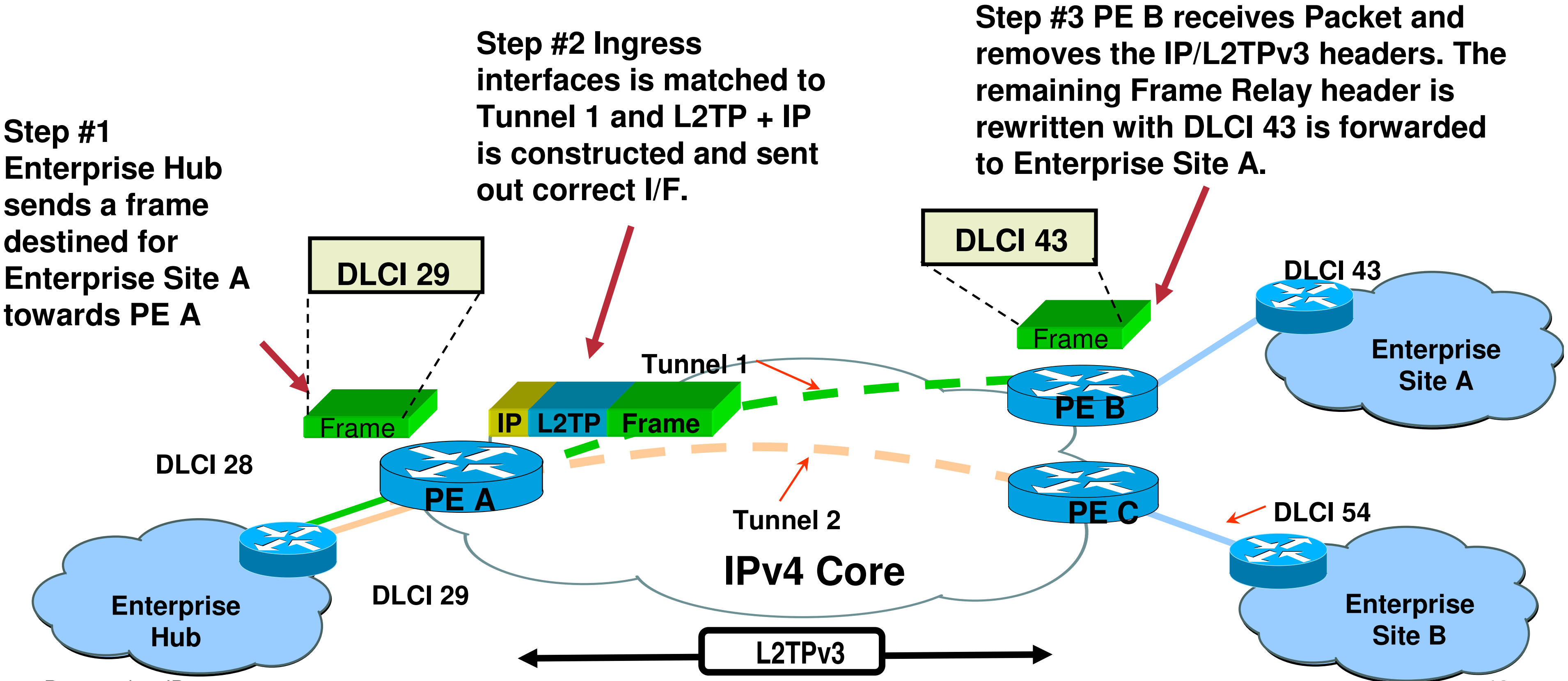
A portion of an HDLC or PPP leased line is emulated over an IP network. To the end user devices, the leased line appears as a single segment.

L2TPv3 – Frame Relay Application Overview

←··············· **Multi-Segment PVC** ···············→

← DLCI → ← PW → ← DLCI →

CE1 ····· UNI/NNI ····· PE1 ······························ PE2 ····· NNI/UNI ····· CE2

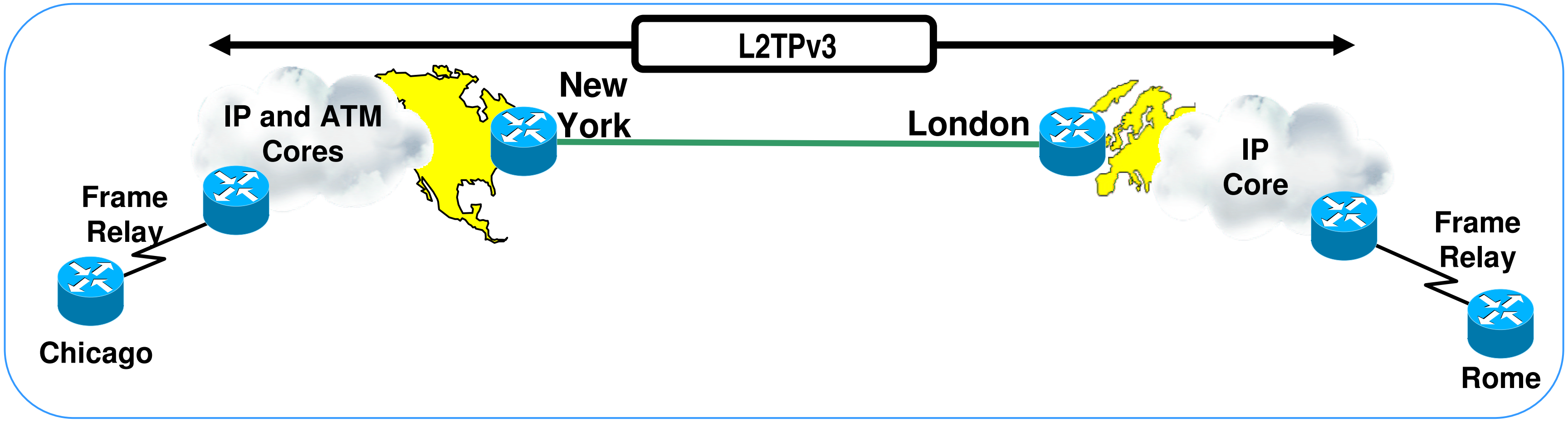


Step #1 Enterprise Hub sends a frame destined for Enterprise Site A towards PE A

Step #2 Ingress interfaces is matched to Tunnel 1 and L2TP + IP is constructed and sent out correct I/F.

Step #3 PE B receives Packet and removes the IP/L2TPv3 headers. The remaining Frame Relay header is rewritten with DLCI 43 is forwarded to Enterprise Site A.

L2TPv3 - Global Reach Services Application



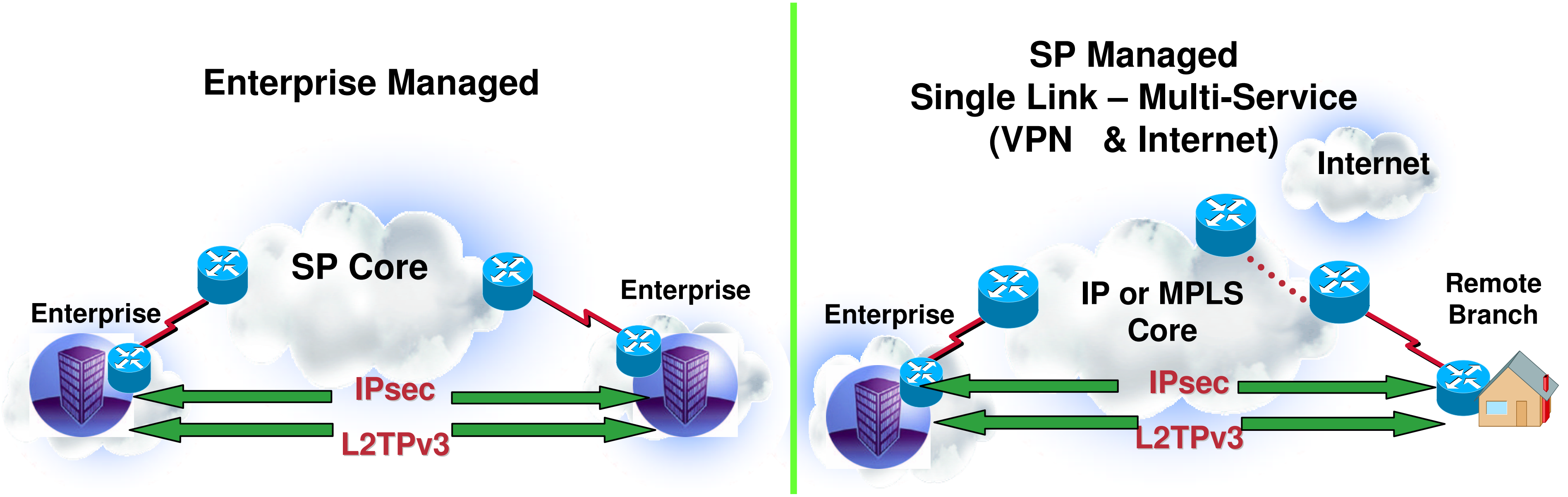
Requirement: Frame Relay connections between Chicago & Rome

Problem: The Service Provider only has an IP Core in London

Solution: Use L2TPv3 tunnels to support L2 connectivity to all sites

Benefits: Time-to-Service, Global Reach, Reduced Cost

IPsec with L2TPv3 Application



- **Requirement:** Establish secure connections between sites
- **Problem:** Customer wants option to manage and outsource selectively
- **Solution:** L2TPv3 connectivity combined with IPsec

L2TPv3 – Summary

- L2TPv3 is a method for transporting a variety of layer 2 circuit types across IP networks
- L2TPv3 is an open standard defined by the IETF L2TP Extensions Working Group
- L2TPv3 has its own in-band Control Connection to dynamically create and maintain sessions.
- L2TPv3 utilizes the experience of a well-established lineage of protocols, including L2TP defined in RFC2661
- Utilization of IP provides global reach for a variety of new L2VPN service offerings.

Agenda – L2TPv3

- Introduction
- Technology
- Applications
- References

References

- IETF Drafts on L2TPv3 Technology

  http://www.ietf.org/internet-drafts/draft-ietf-l2tpext-l2tp-base-11.txt

  http://www.ietf.org/internet-drafts/draft-ietf-l2tpext-pwe3-ethernet-01.txt

- L2TPv3 Technology Deployment

  http://newsroom.cisco.com/dlls/innovators/software_standards/mark_townsley_profile.html

  http://www.cisco.com/warp/public/cc/so/neso/vpn/unvpnst/2tpv3_ov.htm

L2TPv3 Terms & Acronyms

AVP - Attribute Value Pair. Multiple AVP’s make up L2TPv3 Control messages. (Same as TLV’s in Martini specs)

CE - Customer Edge. This is the customer equipment making a direct connection to the Service Provider's equipment (PE).

CIR - Committed Information Rate. In Frame Relay, the minimum average data rate provided to the customer.

Control Connection - A reliable channel that is used to establish, maintain and remove L2TP sessions (directed-LDP in AToM)

Control Message - An L2TP message used by the Control Connection

Data Message - Message used by the data channel

Directed LDP - An extended LDP session used to connected PEs that aren't directly adjacent.

DLCI - Data Link Connection Identifier. A value between 0 and 1023 used to identify a circuit on Frame Relay enabled port.

LCCE - L2TP Control Connection Endpoint. Defined as one end of the L2TP control connection.

LDP - Label Distribution Protocol. RFC3036. One over several protocols available to establish LSP’s.

LSP - Label Switched Path. The path a MPLS encapsulated packets take through the core.

LSR - Label Switched Router. A node participating in an MPLS core.

MTU - Maximum Transfer Unit. Maximum size a frame can be for a Layer 2 specification.

PDU - Protocol Datagram Unit. PDU refers to the Layer 2 data that will be forwarded across the segment (frame).

PE - Provider Edge. This is the a service provider equipment making a direct connection to the Customer's equipment (CE).

L2TPv3 Terms & Acronyms

Pseudo-wire PDU - A PDU sent on the PW that contains all of the necessary elements (control and data) to provide the service.

PSN - Packet Switched Network. Native IP or Multiprotocol Label Switched for this discussion.

PW - Pseudo-Wire. A mechanism that carries essential elements of the an emulated service over the PSN.

PWE3 - Pseudowire Emulation End-to-End (IETF working group devoted to standardization of PWE Services)

PWES - Pseudowire Edge Service (Common attachment technologies, such as ATM, Frame Relay, HDLC, etc.)

Session - Created by an Control Connection. Specifically, a one-to-one mapping of circuit-to-pseudowire.

TLV - Type-Length-Value. Used to define optional parameters used in LDP-Label Mapping messages, comparable to AVP's.

CISCO SYSTEMS

Thank You !

Ray Irani
Cisco Systems